11/5

errors

False Positives: detects a threat when there isn't one.

False Negative: misses an actual threat

Firewalls: examine packets
apply rules
e.g. reject ftp connections by port
reject packets from some network by source IP

Intrusion Detection/Prevention Systems
IDS/IPS

SIEM: security and info event mgmt
- device logs
- packets
- notification
- baselines

(2)

Antivirus - look for some suspicious part of a program

virus has "signature"

check for match

scan for all signatures

quarantan matches

Email:

sender policy framework:

check if src IP addr. is from sender's domain

e.g. gettysburg.edu

should be 138.234....